陸、 專題報告：網路對於洗錢及資恐犯罪之促發作用

內政部警政署刑事警察局　科長李維浩
股長王啟秀

一、 前言

利用科技做為金融犯罪的利器，在過去10年中逐漸成長。這也與資訊與傳播科技多元利用技術的進步有關，例如網際網路及社群媒體科技及相關的金融平臺等技術。以網路進行洗錢或資恐活動的方式，可以在二個面向上被理解：利用網路洗錢的前置犯罪(網路犯罪)以及利用網路作為犯罪所得或資恐行為的清洗工具(網路洗錢)。

網路犯罪是一種可以使犯罪不斷演化的領域。犯罪行為人在此領域中可以使用網路的匿名性，速度性及便利性來達成各種形式的非法行為，且在具體或虛擬的模糊界線下，對全球的被害者造成實際威脅並導致嚴重損害，例如在未經授權狀態下將銀行裡的資金移除或進行提款卡詐欺等行為。

在亞太地區，網路詐欺是一種特別且普遍存在的威脅。在最近所公布的一份研究報告指出，2017年亞太地區的詐欺犯罪中，有關網路犯罪部份與去年同期相比成長了35%，特別是在犯罪人假冒真實持卡者身份進行信用卡欺詐及付款詐欺部分。該報告也特別指出，全球的網路犯罪自2015年後期開始迄今，幾乎成長了百分之百，而其主要的原因就是從2017年晚期所發展出的人頭帳戶詐欺，貢獻了30%的成長率。

2018年APG的洗錢態樣報告因之聚焦於認識網路犯罪，並將網路洗錢犯罪之犯罪所得進行洗錢等相關議題納入新興的洗錢風險及趨勢。以下詳細說明該部分之重要內容及相關案例，並具體建議因應作為。

二、 FATF 對於打擊洗錢資恐及網路犯罪之新措施

防制洗錢金融行動工作組織準則包含了有關打擊網路犯罪的廣泛工具。特別是將洗錢及資恐犯罪行為化的部分，可適用於各層面打擊網路犯罪的許多犯罪行為類型

（一） 資助恐怖主義(包含恐怖主義本身)：恐怖主義在網路及社群媒體上隨處可見，由其是欲提供金援予位於海外的恐怖份子或其組織的支持者更可見一般。

（二） 性剝削(包括兒童性剝削)：兒童性剝削行為包含在網路上進行製作，傳播及散布兒童性剝削之內容，進而藉此產生犯罪所得，其

每年產值可高達數十億美元。而利用網路傳播科技(ICT)來進行商業化的兒童性剝削，除可讓犯罪者降低其製造及散布該內容的成本進而增加其潛在獲利外，亦可讓大多數的潛在客戶在線上進行存取。

（三） 非法運輸：防制洗錢金融行動工作組織準則所指非法運輸，係有關於麻醉管制毒品及精神藥物，非法武器以及其他遭竊物品之非法運輸等。而上述毒品，武器及竊盜等物品亦均可藉由網路方式進行販賣，或以更匿名地方式透過暗網(Dark Web)進行。

（四） 詐欺與身分竊盜：這些犯罪已經在網路上存在了一段時間，也是各會員國內司法管轄上普遍面臨的爭議問題。

（五） 搶奪或竊盜：網路傳播科技也會促進新形態的搶奪或竊盜行為。

（六） 恐嚇取財：恐嚇取財也可能透過網路傳播科技方式進行，但犯嫌向被害人取財方式也可能採傳統非網路模式進行。然而網路科技也可能使恐嚇取財以新的方式進行，例如透過勒索軟體。勒索軟體是一種惡意程式軟體，作用在於鎖住硬體或惡意加密後阻止使用者存取資料庫資料，使用者於付出贖金後方能解鎖。勒索軟體攻擊通常也會用來取得加密貨幣，例如比特幣，使其位於特定 IP 位址的帳戶遭到解鎖。

FATF關於國際合作的第36項建議，鼓勵各國應批准並執行2004年7月的網路犯罪公約（又稱為布達佩斯網路犯罪公約或是布達佩斯公約）。這項公約是第一個尋求通過協調各國法律、改進調查技術和加強各國間合作打擊網路犯罪和電腦犯罪的國際條約。FATF還發布了關於商業網站和網際網路支付系統的洗錢及資恐漏洞的報告（2008年）。該報告強調了以下內容：

（一） 商業網站和網際網路支付系統的脆弱性包括：用戶匿名、有限的人為干預、交易速度快、交易量大、非面對面註冊、存在於國際間、有限的司法管轄權限，傳統金融機構於監控和檢測可疑的金融交易時存在困難，其結果導致每當網際網路支付服務提供商被使用時，他們檢測可疑金融交易的能力可能受到影響。

（二） 許多有關非面對面的商業、金融交易以及貿易洗錢之洗錢/資恐風險，也適用於網際網路支付系統和商業網站。大部分在線支付係透過銀行賬戶或信用卡；那些交易已經涉及客戶識別，報告義務和交易記錄保存的過程。由於低價值交易並不一定與低風險相關聯，因此這些交易仍然受到金融部門的監管控制。

（三） 當涉及到與非面對面相關的風險及用戶可能的匿名性時，為了幫助

商業網站和網際網路支付服務提供商減少犯罪活動的風險，需要在線身份驗證解決方案，例如在某些司法管轄區使用的電子身份證。

（四） 如果網際網路支付服務提供商充分監控其客戶的財務交易，監控客戶交易資料的差異並採取相應行動，則客戶們與商業網站和網際網路支付服務提供者間雖然一開始缺乏面對面的聯繫，也許不會構成問題。

（五） 有效比較網路零售、支付服務商及離線零售、支付服務商間的反洗錢/反資恐義務，至關重要。

（六） 網際網路支付服務提供商及不同司法管轄區的商業網站對打擊洗錢和資恐的努力，雖然不會被隱私權相關法律所阻礙，但是這些法律可能會干涉服務提供商之間於交換可疑洗錢/資恐之客戶資訊的數量。

在2013年，FATF發布了一份報告：「預付卡、移動支付和網際網路支付服務的指南——以風險為基礎的方法」。 全球「新型支付產品和服務（NPPS）」功能增加，業務快速增長，越來越多人使用此一服務。在確保這些產品和服務不被用於洗錢及資恐之目的時，此一快速增長的事實已經對各司法管轄區和私營機構，產生了障礙。針對「新型支付產品和服務（NPPS）」，各司法管轄區正致力於制定並實施反洗錢/反資恐的規範，方法是：

（一） 解釋「新型支付系統如何運作？」、「哪些實體涉及提供新型支付產品和服務？」、「他們的角色及行動方式」。

（二） 審查涉及提供新型支付產品的實體中，哪些在 FATF 的建議規範之內（例如屬於 FATF 所定義的金融機構）

（三） 預估提供新型支付產品和服務的風險。在預估風險時，同時考慮所有有關的風險及降低風險的措施。

（四） 考量此類規範對於新型支付市場的影響。包括此類規範是否影響到金融包容性（final inclusion），以及是否對金錢存款流動至正規金融機構有正面影響。

根據NPPS指南，FATF在2014年發布了一份報告「虛擬貨幣：關鍵定義及潛在的反洗錢/反資恐風險」。為了瞭解並解決有關網路支付系統的反洗錢/反資恐風險，這份報告提出了一個概念框架：虛擬貨幣。具體而言，本文提出了一個通用的詞彙定義，基於不同的商業模式及營運模式，闡明了虛擬貨幣是什麼以及其種類，並闡明了虛擬貨幣系統中的典型參與者。2013年NPPS特殊類型虛擬貨幣指南也

在第四節（A）段中列出了風險因子，用以識別潛在風險；描述一些執法部門近期就調查虛擬貨幣的努力；並提供了一些司法轄區對虛擬貨幣現有監管模式的例子。

在2015年，FATF發布了「虛擬貨幣指南——以風險為基礎的方法」。此一指南係FATF所採取的階段性方法中的一部分。此前FATF已經發布了2014年的虛擬貨幣報告，還有結合了風險與最佳實踐的2013年NPPS報告。事實上，為了保障全球金融體系的誠信不受犯罪及網路洗錢等網路犯罪傷害，虛擬貨幣支付產品與服務（VCPPS）的發展，以及VCPPS與NPPS甚或傳統銀行服務之間的交易，對這份報告的需求因而攀升。該指南的重點在於，在十字路口提供了一個通往受監控的金融體系的成功道路，特別是可兌換的虛擬貨幣的兌換商。

三、 現階段打擊網路犯罪之努力及挑戰

以網路促發的洗錢，資恐犯罪及網路犯罪近年來已引起國際矚目之焦點。在許多司法管轄，區域性及國際層級上所進行的活動，期能對於網路犯罪本質，防制策略，偵查及起訴犯罪行為人等議題上獲得更多了解。

（一） 加密貨幣規範

歐洲理事會網路犯罪公約(也稱為布達佩斯公約Budapest Convention)是目前處理國際網路犯罪主要工具。它幫助締約國協調國家法律，提升調查技術並加強國際合作，同時強調目前有關虛擬貨幣的最關鍵考量，在於是否接受反洗錢與反資恐相關規範及監督。

馬來西亞已經要求虛擬貨幣兌換商實施反洗錢/反資恐必要作為。在其「2001年打擊非法洗錢及資恐行動」的清單中，這些兌換商的實體均為申報機構。虛擬貨幣兌換商須執行針對洗錢/資恐相關風險的有效措施，並提高虛擬貨幣活動的透明度。此外，這些虛擬貨幣兌換還必須提供有關其進一步的業務資訊和活動，並每月提交虛擬貨幣交易報告。

澳大利亞也透過「2006反洗錢及反資恐法」及依此頒布的「2018兌換虛擬貨幣反洗錢/反資恐登錄政策原則」，對虛擬貨幣兌換商實施了反洗錢/反資恐的要求。虛擬貨幣交易商必須有一個適當的反洗錢/反資恐計畫，向澳洲交易報告及分析中心（AUSTRAC）登錄，報告可疑洗錢交易並維持足夠的交易紀錄。

（二） 對於各國司法管轄權的挑戰

由網路促發的洗錢及資恐犯罪對於各國的司法管轄帶來許多挑戰，包括:

1. 各執法機關間缺乏調查網路犯罪的專家。而國內負責調查網路犯罪以及洗錢與資恐犯罪的執法機關間如果又沒有充分溝通協調的話，狀況將更形複雜。

2. 因法律增修的速度遠不及科技的變化，致使網路犯罪的立法亦付之闕如。而當網路威脅如同科技發展般地快速演進之際，商業秘密竊取技術也會一邊發展，竊取者自身一邊進行改變。

3. 其他的挑戰包括許多網路犯罪的本質上即具有跨國特性。某人可以在某國司法管轄領域內犯罪，但卻利用位於另一司法管轄領域內的網路平臺，對在第三國司法管轄領域內的被害人進行犯罪。偵辦網路犯罪與相關的洗錢或資恐犯罪需要強力的國際合作，此合作不僅指地理疆域上的司法管轄權的連結合作，更需要拓展強化網路傳播科技上的合作與連結。正因司法管轄權界線在網路空間中，其本質上就會產生漏洞，所以更突顯打擊網路犯罪之國際執法協調與合作重要性。

4. 網路犯罪及網路洗錢及資恐犯罪的偵查亦須與私部門進行緊密的合作。私部門在其網路基礎設備營運上，並不常與執法機關間進行安全與合作列為優先考量。如前所述，網路犯罪的跨國性質通常也拘束了司法管轄對於外商公司的執法能力。相反的，用合作代替處罰的方式以獲得私部門的協助，像是社群媒體與電信公司，將更蒙其利。

5. 對於線上轉帳及交易的安全性缺乏信心的狀況下，將會限制該司法管轄範圍內的金融交易數量，使得客戶轉移至其他較安全的市場進行交易。

四、 各國偵辦數位洗錢（藉由網際網路洗錢/資恐)之案例

（一） 孟加拉

1. 案例1

通過對社交媒體的定期監控工作，「社交媒體監控小組（SMMST）」發現了一個名為「X」的帳號。這個帳號被用於宣傳激進的意識形態，鼓勵其他的社交媒體用戶參與持續的抗爭。該帳戶還募集用以摧毀世俗孟加拉國的資金，以求建立政教合一的「哈里發（Khilafah）」。

在此背景下，「社交媒體監控小組（SMMST）」乃向相關社交媒體

公司尋求幫助，以確定該帳號所有者的身分。依據社交媒體公司提供的資訊以及追查行動電話之後，「社交媒體監控小組（SMMST）」因而逮捕到躲藏在這個帳號背後的人。在調查期間，「社交媒體監控小組（SMMST）」瞭解到X是一虛構的名字，實際上則由「Y」這個人於社交網站上運行這個帳號。調查人員還瞭解到，Y為孟加拉政府指定實體「安薩利艾爾伊斯蘭孟加拉團隊（ABT）」的活躍成員。

孟加拉金融情報中心（BFIU）從調查權責部門獲得有關Y的資訊，並搜索了Y在金融業的帳戶。搜索結果發現他有三個銀行帳戶和多個行動電話金融服務（MFS）帳戶。這三家銀行的帳戶都確認了此客戶有網上業務和聯盟行銷。但是，不管是在開戶申請書（Account Opening Form, AOF）或是瞭解你的客戶（KYC）的簡介中都沒有記下任何與其交易過的網上業務實體、合作夥伴實體、帳戶或網頁的名字。這些帳戶上有來自不同司法轄區的零星小額現金存款。行動電話金融服務（MFS）帳戶有頻繁的交易，主要是現金交易；這些帳戶使用了全數交易限額。所有的帳戶都保持著最低餘額。

根據 「2009年反恐行動法」及「2006年資訊技術與通訊行動法」，已對此人起訴。目前，調查人員正在進一步調查以確認他的共犯。

2. 案例2

有一個臉書網頁係以孟加拉高級官員的名義創設。在此網頁中貼了一些關於政府向失業者提供財政援助的帖子。為了取信於人，這個網頁使用了「遠離恐怖主義，回歸正常生活：政府向失業的赤貧人群提供財政援助」等標語。也使用了一些政府官員送交支票的典禮的照片。這個網頁提到一個電話號碼和電子郵件地址，並指示對此一活動感興趣的人可聯繫他們以獲取金融援助。

有些人被此一臉書上的帖子所吸引，聯繫了上述電話號碼和電子郵件地址。然候他們被電子郵件通知已被選中為政府援助的對象，並且政府援助的支票將很快送交給他們。這封電子郵件還指示他們預先將25%的批准金額存入該援助計畫專案主任的銀行帳戶，以作為安全金。此一銀行帳戶的戶名是「J女士」。有些人將錢存入此一帳戶中，但沒有收到所謂政府部門的任何回應。

這個議題引起相關部會的注意，他們將此一問題向執法部門、相關銀行及中央銀行報告。在被告知後，銀行提交了可疑交易報告（STR）；中央銀行的各個部門則轉知孟加拉金融情報中心（BFIU）。BFIU調查發現，有一群人涉犯詐欺罪，他們運用上述的臉書網頁及銀行帳戶來詐騙。有60萬塔卡（約21萬新臺幣）存入了

這個銀行帳戶。這些存入的錢在很短的時間內就被提領一空。領出的錢有一部分又轉存到這家銀行的其他帳戶。詐欺集團成員的這兩個銀行帳戶以及一個行動電話金融服務（MFS）帳戶內有餘額20萬塔卡（約7萬新臺幣），均依2012年洗錢防制法（MLPA）予以凍結。有關本案的分析報告已經分送予執法部門。

（二） 汶萊

1. 盜用身分

犯罪者使用被害人的姓名或身分來犯罪。身分識別的細節包括：姓名、國家身分編號、金融資訊〔帳號及用戶個人識別號碼（Personal Identification Number, PIN）〕。犯罪者透過社交工程（如以電子媒體網路釣魚、語音電話、即時簡訊平臺）等不同方式以取得這些身分資料。這些身分資料被用來進行詐欺，包括信用卡或是金融卡詐欺，以及未經授權的網路銀行轉帳。

2. 網路詐騙

犯罪者使用社交媒體獲得受害者的信任，繼而以提供產品、服務、商業投資、愛情（romance）等方式詐騙被害者。例如浪漫騙局（a romance scam），又稱為包裹騙局（a parcel scam），這是一種高級的費用詐欺，犯罪者會以某些理由要求被害者送錢，理由例如：為了確保他（即犯罪者）能安全無虞的旅行到被害者的司法轄區內（與其相見）。

3. 性勒索

被害人（通常是年輕人）遭到設計而以視訊聊天的方式進行性行為。被害人為了避免這些性愛影片上傳及散佈，被迫支付費用。

（三） 斐濟

1. 為犯罪而進修

曼吉特·辛格（Manjeet Singh）和傑尼爾·蕭達利（Rajneel Chaudary）是在南太平洋大學（USP）就學的朋友，他們密謀非法取得朋友、同事的網路銀行資料，以竊取資金。曼吉特·辛格知道房東把他所有的銀行帳戶資料都放在什麼地方，他運用了這些房東的資料登入其網路銀行。然後曼吉特·辛格從房東的帳戶進行了三次轉帳，轉到自己名下的帳戶、傑尼爾·蕭達利的帳戶，還有艾爾提·達夏娜·雷蒂（Arti Darshana Reddy）的帳戶。艾爾提·達夏娜·雷蒂是曼吉特·辛格的朋友，他曾用她的帳戶支付學費。資金帳到艾爾提·達夏娜·雷蒂的帳戶後，曼吉特·辛格用艾爾提·達夏娜·雷蒂的

ATM卡把錢領走。

傑尼爾・蕭達利則拜訪了一家銀行分行，透過「要把錢存入某個帳戶」的幌子來調查該被害人帳戶的資料。他因而取得了個資明細並進入被害者帳戶。然後曼吉特・辛格從該被害人的帳戶進行了三次網路銀行轉帳，合計4340斐濟元（約新臺幣6萬3千元）。

曼吉特・辛格在2017年3月被判三項洗錢罪名成立，同年4月宣告有期徒刑9年。另外傑尼爾・蕭達利也在同年4月承認三項洗錢罪名，宣告有期徒刑8年。

這是首宗因國內的網路犯罪而導致2次洗錢犯罪的案例。銀行系統的勾串和操縱的情形顯而易見，這對斐濟的網路銀行系統帶來廣泛的影響。

（四） 日本

日本金融情報中心從其策略分析中發現，已經有許多銀行帳戶匯入網路賭博犯罪之犯罪所得。有關此類犯罪行為資訊亦轉送予執法機關。

（五） 中國澳門

司法警察局在2017年8月受理了一起詐欺案件，據這個案件的女性被害人所陳，她曾被騙了一大筆錢，並在2016年時將案件經過情形上傳到網路上。被害情形上網後，她和一名自稱是同案被害人的的犯嫌成為朋友。上述犯嫌透過通訊軟體接近被害人，他又宣稱自己曾是一名高階警官，可以透過法院的關係以合法方式優先拿回她損失的錢。在兩名假扮為法院職員的詐欺集團成員的指示之下，被害人隨後以電匯方式將錢存到指定的帳戶超過20次，合計63萬澳門幣（約新臺幣240萬元）。最後她終於意識到自己被騙了，並向警方報案。

另一個類似案件的女性被害人在2017年11月向司法警察局報案，她陳指與一名當地男子有借貸關係，在2015年時借給他港幣55萬（約新臺幣214萬元）之後就與他失去聯繫。有一名宣稱是放貸者的犯嫌於2016年10月31日透過網路社交平臺與被害人取得聯繫。他說願意償還這筆借款，但要求她先支付一筆手續費以解凍他的銀行帳戶。被害人隨後收到了3名假冒檢察官辦公室及法院職員的人以手機通訊軟體傳來的訊息，要求她以人工轉帳的方式來處理這筆手續費。她最後被騙了港幣1000萬（約新臺幣3千9百萬元）。

司法警察局確認了上述案件的涉案犯罪來自同一個詐騙集團。2017

年11月11日，在北區和中區的幾個公寓中逮捕了男女共8名的嫌犯。另外還扣押了犯罪證據及港幣24萬（約新臺幣93萬元）的不法所得。

調查顯示，其中一名被逮捕的女性嫌犯是這些案件的首謀，而其他的犯嫌則假冒司法機關的工作人員以進行詐騙。首謀犯嫌使用自己及其他集團成員的銀行帳戶來收取、提領不法所得，迂迴移轉這些錢，最後存入他們的海外銀行帳戶。

司法警察局以詐欺及洗錢的罪名，將這8名嫌犯移送檢察官辦公室，並繼續追查其他涉案人員及不法利益。

（六） 馬來西亞

1. 商務電子郵件詐騙（BEC）

A先生是其所在機構的一名資深會計師，他收到了一封列印出來且親手送交的電子郵件之指令，該指令中以一份據稱為其上司送來的發票為憑證，其涉及變更受益人的120萬美元預定付款之銀行資訊明細。原本預定的受款帳戶是位在A司法轄區，被變更為位於B司法轄區的另一個銀行帳戶。這兩個帳戶的所有人姓名完全相同。

A先生確信手中的這一指令，製作了一份新的電匯表格更改受益人的受款帳戶為新的帳戶，這份新的電匯表格也被相關上級人員所批准。新的電匯表格被送到銀行並開始匯款給受益人的新帳號。

當日稍晚，A先生收到一位上級主管的電話，這位主管意識到這個新電匯是詐欺。A先生被告知，其上司與受益人間的電子郵件往來及預定接受的金額已經被一個未知的犯罪者所截獲，並變更了受益人的銀行資訊明細。警方提出了報告，並立即下令收回這筆資金。

在本案中，這筆電匯因金融情報中心及不同司法轄區（包括被害人的司法轄區及B司法轄區）相關執法部門的迅速行動，得以成功凍結。這得益於艾格蒙組織的BEC快速回應計畫。

一般而言，BEC案件會出現下列癥兆：一、建立/運用與被害人的公司名稱極為相似的公司名稱，包括知名的國際公司；二、吸金的金額不會太高而是在公司的正常營運範圍內，以避免遭到被害人的懷疑；三、交易的指示方式不尋常；四、使用偽造的文件；五、資金會立即從帳戶中提領走，可能是透過現金提領或是轉帳到其他代理人的帳戶；六、不一致的帳戶行為，包括移轉資金目的之變更。

（七） 紐西蘭

紐西蘭警方近來發現一宗有關利用越南人臉書社群網頁來找尋一些

不會被懷疑的對象來幫助洗錢，而這起案件實質上就是負責古柯鹼進口的跨國犯罪網絡。

當警方調查這起大量古柯鹼進口案件時，監控到一名犯嫌與一名已知的洗錢者見面。這位男性犯嫌將一袋現金交給另位女性，該女性隨後即至某銀行外頭與某人碰面。後來隨有100萬紐幣被存入該銀行洗錢者的帳戶。

當該洗錢者被逮捕後，該女子解釋她是想將一筆錢，在不透過西聯匯款或讓銀行收取手續費的方式下，從越南轉入紐西蘭，而將該訊息張貼在當地越南社群臉書留言牆的網頁上。後來有某位男性回復並安排她與他的母親見面，聲稱他的母親也想弄一筆錢回越南。當這兩位女人在銀行碰面後，該洗錢者的母親同時在越南的某銀行將相當於100萬紐幣金額存入越南銀行帳戶。

在接下來的詢問中發現，最初的那一位男性犯嫌與他的母親已經與8個其他不同人分層洗錢且彼此不曾互問過任何問題，因為這在洗錢過程中是很正常的。

最初男性洗錢車手雖被控洗錢罪，但是隨著洗錢車手遭利用範圍程度愈臻明確，該洗錢罪名最後仍遭撤銷。儘管如此，紐西蘭警察資產追回小組仍然將該100萬紐幣視為犯罪所得進行管制。

（八） 新加坡

1. 國際轉帳/匯款詐欺(洗錢車手)

在2012年初，新加坡警察局商業事務部發現有一犯罪趨勢，即犯罪嫌疑人以駭客手法入侵被害人電子郵件後，假冒被害人名義指示其存款銀行將資金轉匯至另一新加坡銀行帳戶。在其他案例中，被害人遭詐欺的手法，包括國際型的愛情詐騙，讓被害人心甘情願依犯嫌指示將錢匯款至其指定帳戶中。

新加坡警察局商業事務部調查後發現，在海外有一群犯嫌專門在處理這些遭詐騙後轉移的贓款，且與實際從事詐騙的犯嫌並無直接相關。這些銀行帳戶持有人多是新加坡在地人且與該犯罪集團成員交好，而主要係透過社群網路認識。這些持有新加坡當地銀行帳戶者即為我們所熟知的「洗錢車手」，不論他們是否知情，均會按犯嫌指示接收來自犯嫌帳戶的匯款，然後再將該筆資金轉匯至其他地方，通常是海外帳戶。而這些「車手」亦就其角色分工來收取一定的傭金。

以下列表內詳列外國被害人的帳戶數目，新加坡警察局商業事務部

得以透過與外國執法機關合作，成功將被害人帳戶轉帳至新加坡的犯罪所得扣押之情形。

新加坡警察局商業事務部查扣銀行帳戶及犯罪所得數目

年份	2012	2013	2014	2015	2016	2017
外國被害人帳戶數	129	264	148	64	37	44
從被害人帳戶因錯誤詐欺而轉至新加坡帳戶之金額(單位：百萬美元)	24.6	31.5	14.9	6.67	3.81	5.41
遭查扣犯罪所得百分比	11	18	15	15.6	25.1	36

新加坡在打擊此類犯罪趨勢所付諸努力是成功的，特別是從報告中的數字顯示，新加坡「洗錢車手」透過國際轉匯所得的詐騙所得金額有實質上的降低。從2013年最高峰的264個外國被害人帳戶數，到2017年只剩44個外國被害帳戶，整體下降83.3%。而自2015年開始數字持續維持下降趨勢。這些成效多歸功於新加坡新加坡警察局商業事務部採取多管齊下的做法：一、與相關機關即時分享情資，如外國的金融情報機關以及企業夥伴；二、與不同國家的執法機關進行緊密的合作，以鑑別出被害人的錢是如何遭詐騙而轉匯至新加坡，進而在新加坡展開司法互助調查程序；三、與新加坡檢察總署合作共同嚴正執法，打擊洗錢車手；四、強化犯罪預防與公眾教育領域。

（九） 泰國

1. 線上樂透彩詐欺

W先生從中東地區某國家與泰國洗錢防制辦公室聯繫，請求該辦公室立刻准予放行一張由國際快遞通運公司所寄送之支票。該名男子聲稱這張支票是在雅虎公司所贏得的樂透彩券，泰國洗錢防制辦公室無權扣押該張支票。經該男子與洗錢辦公室人員聯繫後方得知，他係遭偽稱為雅虎公司樂透銷售部協調員所詐騙。

在W先生與泰國洗錢防制辦公室聯繫前，已透過西聯匯款方式將650美元轉匯給S先生，以該取得樂透彩中獎支票。而該辦公室的名銜竟也被用來增添該詐術的可信度。

2. 社群媒體詐欺

某女性受害人透過臉書與外國人P進行聯繫。她遭詐欺後將11筆金額

匯款至該犯嫌所開設的數個銀行帳戶中，總損失超過1百萬泰銖。(相當於美金3萬5千元)

該名被害人將其中一筆35萬泰銖(相當於1萬美元)轉入至Y小姐在T銀行開設的帳戶中(聲稱是P先生的生意夥伴)。而在這之前，該銀行早就偵測到該帳戶的異常交易狀況並通知各分行將該開戶人相關資料提交總行，俾進行加強盡職調查程序(EDD)。

五、 結語

由各國案例可發現，無論是各類型前置犯罪抑或是其衍生之洗錢犯罪，其結合網路科技之便利性、隱密性已是常態。除犯罪類型及手法不斷改變外，此一結合已明顯對刑事偵查造成衝擊，增加偵查人員於案件偵查及蒐證之困難。

未來各執法機關宜持續就新興科技犯罪手法態樣、社會環境變遷性及符合法律規定等全盤考量，加強科技偵查人才之培訓，積極研析可能突破之技術瓶頸，以解決新興科技所帶來之犯罪問題。此外，網路世界無遠弗屆，偵辦案件之跨境合作尤其是國際間之情資交換愈形重要，除依循正式之外交合作管道如司法互助外，鑑於我國國際處境之特殊情形，各執法機關宜本於自身之職掌，不拘形式爭取各種合作可能性，俾實質提高情資交換之效率。